APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,574	12/09/2004	Brian Albert Wittman	PU020277	1365

7590   04/13/2009

Joseph S Tripoli
Thomson Licensing Inc
PO Box 5312
Princeton, NJ 08543-5312

EXAMINER
VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
04/13/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>31 March 2009</u>.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1,6-9,16 and 18-35</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1,6-9,16 and 18-35</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/517574 is presented for

examination by the examiner. Claims 1, 6-9, 16, and 18-35 are pending. Claim 27 has

been amended.

Response to Amendment

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly
claiming the subject matter which the applicant regards as his invention.

Claims 25, 29, and 33 are rejected under 35 U.S.C. 112, second paragraph, as

being indefinite for failing to particularly point out and distinctly claim the subject matter

which applicant regards as the invention.

As per claims 25 there seems to be a contradiction in the way the invention is

functioning with respect to how it is disclosed in claim 23. In claim 23, as Examiner

interprets, when a rule is a broken the particular user discernable indicator give

affirmation that traffic is being filtered. When a threshold of rule is broken the respective

class indicator goes off. So two things are happening, independently from one another.

The particular indicator depends on any traffic filtering. The respective indicator

depends on a rule threshold. It appears that the particular indicator always goes off

anytime a packet is deemed to have broken any rule. If this indicator's purpose is to alert the user whenever data is being filtered, then there seems to be some discrepancy with how this particular one operates. Claim 25 is rendered indefinite because it states that the only indicator that will go off when a threshold is not exceeded is the respective indicator. Examiner contends that according to claims 23, the particular indicator would be contemporaneously going off as soon as the first packet broke a rule regardless of the threshold. In reading claim 25, the question, is how could (why would) only one indicator go off if the threshold is not exceeded. This appears to also be in conflict with the purpose of the invention. Namely that a user would still want to know anytime filtering is being performed.

Claims 29 and 33 share this same problem with their respective parent claims as interpreted by Examiner. Appropriate correction is required.

Response to Arguments

Applicant's arguments filed 3/20/09 have been fully considered but they are not persuasive.

With respect to the 112 arguments, Examiner respectfully disagrees with the interpretation of the claimed language. It appears the claims do not support or can be interpreted in a manner inconsistent with the Applicant's position. Applicant states that the particular one is governed by the threshold. Claim 23 reads,

"the particular one of the plurality of user discernable indicators being associated with an affirmative status that filtering is being contemporaneously performed for any of the packets that violate the one or more rules".

Thus, for any violating packet, the particular one is triggered. The method proceeds by the filtering any of the packets that violate the one or more rules. Examiner interprets that as the particular one is triggered. We are talking about a particular user discernable indicators, so its inferred that the trigger is user discernable. Then the rest of claim 23 reads,

"wherein the particular one of the plurality of user discernable indicators is concurrently triggered, along with the respective one of the plurality of user discernable indicators, to indicate that the filtering is being contemporaneously performed".

Here the particular one has been triggered along with the respective one. And why (or rather when) was the respective one triggered?

"only when a number of the packets that violate the one or more rules exceeds a pre-specified threshold".

So the claim can be interpreted as the respective one is governed by the threshold. Applicant is interpreting that last clause to refer back to the particular one. It would be clearer if it is intended that the particular one is governed by the threshold to explicitly define that limitation when the particular one is defined and not attached to the end of the claim after several prepositions. Because the limitation can be interpreted two ways, this constitutes indefiniteness in conjunctions with the dependent claims which state the respective one is the only trigger which goes off when the threshold is

not exceeded. The claim should be arranged so that it distinctly points out the invention
and not leave the limitation open to interpretation.

With respect to the 103 rejection, Examiner respectfully disagrees that the
combination of ZoneAlarm and Hrabik do not render obvious the invention of the
independent claims. Applicant states the Hrabik does not teach rules, classes, or
priority level. First of all, ZoneAlarm teaches rules and classes. Hrabik was relied upon
only to teach prioritizing the zones. Zones too are disclosed by ZoneAlarm. For
example ZoneAlarm teaches an Internet Zone (inherently untrusted) and a trusted Zone
(inherently trusted). ZoneAlarm teaches a layered approach to security but not
necessarily hierarchical. Each of the classes (incoming, outgoing, privacy, mode)
having their own rules can be separately applied to the zones (Internet, trusted). Hrabik
explicitly teaches an admin may be more concerned with that is going on in one zone
than another. For example the admin may be more cautious about what is going on in
the Internet zone. Prioritizing the classes of that zone give those rules which govern
that zone more priority over the rules in other classes of other zones. For another
example, an admin may be more concerned with the zone (subnet) that the financial
server is on. So all alerts from that zone could be preferential treatment to invoke the
fastest possible response. All of the rules, classes, and triggers are taught by
ZoneAlarm. Hrabik teaches the idea that an event can be more important depending on
where it occurred in the network. The event is clearly the breaking of a rule because
the rule defined what the event is. Without a rule about some type of event, the event
goes unnoticed if the system is not capable of detecting it. Hrabik also teaches the idea

of prioritizing types of attacks because some network devices are more susceptible to certain types of attacks (0059). This bodes well with the teachings of ZoneAlarm. Types of attacks are equivalent to the classes of ZoneAlarm. It makes sense that some devices are not equally susceptible to all classes of attack. Therefore if certain rules (corresponding to events detected) were given more priority, the classes they belong to would follow the same prioritization.

The combination of the prioritizing of Hrabik within the system of ZoneAlarm does not in any reduce the functionality of ZoneAlarm in such a way. The combination only adds to the security of the system which one of ordinary skill in the art would obviously want to achieve. Prioritizing the rules and classes simply gives the user a more efficient means of monitoring and response. Knowing the critical events which are happening on the network is the most important information when it comes to safeguarding the resources.

With respect to the dependent claims only those which presented a real argument will be address. Merely saying a reference does not teach the entire claim without saying why, is not an appropriate response. Moreover, it is not clear what the intention of the response is because in referring to claims 20-35 because the applicant has referred to them as new claims. These claims have been previously presented and examined and thus are not new.

In response to Hrabik not teaching determining if a first threshold level of a rule is in violation before triggering the response, Examiner cites 0059 for support. Hrabik teaches looking for events exceeding predetermined thresholds, combines this

information about the similar events and produces a security ticket (user discernable

indicator). It is obvious that this occurs not prior to the threshold being exceeded

because then what would be the point of putting them all into a single concise ticket for

the user.

In response to applicant's argument that Examiner's reasoning to combine Hrabik

and ZoneAlarm is different than Applicant's reason for combining, the fact that applicant

has recognized another advantage which would flow naturally from following the

suggestion of the prior art cannot be the basis for patentability when the differences

would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. &

Inter. 1985).

With respect to claim 35's arguments, ZoneAlarm the primary relied upon

reference is a software tool aimed for end-users. The main advantage of the software,

is that it gives an end-user the power, flexibility, and manageability that a system admin

has for a larger scale network. It is simple enough for a single end-user to operate yet

powerful enough to safeguard the user's resource from a single point of operation.

Many of the features of ZoneAlarm are taken from the vast tools which system admin

have had but simplifies them into one package. Bringing over one more tools from the

admin domain is well within the ordinary capabilities of one of ordinary skill in the art.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 6-9, 20, 21, 23-30, and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable ZoneAlarm publication by Ash Nallawalla hereinafter ZoneAlarm in view of USP Application Publication 2002/0178383 to Hrabik et al hereinafter Hrabik.

As per claim 1, ZoneAlarm teaches an apparatus [PC with ZoneAlarm is installed] adapted to communicate via a network, comprising:

a firewall [ZoneAlarm] including a set of rules for identifying packets associated with inappropriate activity, the rules in the set being separated into a plurality of classes; and an indicator device for providing a plurality of user discernable indicators [ZoneAlarm alerts], wherein each of the plurality of user discernable indicators is associated with a different one of the plurality of classes [classes are outgoing traffic, incoming traffic, identifying/privacy data, and malicious code], and wherein a respective one of said plurality of user discernable indicators is triggered if one or more of the rules corresponding to one of said plurality of classes associated with the respective one of said plurality of user discernable indicators is violated [see alert from figure 3 and figure 7].   ZoneAlarm teaches sets of rules into a plurality of classes and an indicator device

for providing a plurality of user discernable indicators, wherein each of the plurality of
user discernable indicators is associated with a different one of the plurality of classes,
and wherein a respective one of said plurality of user discernable indicators is triggered
if one or more of said plurality of rules corresponding to one of said plurality of classes
associated with the respective one of said plurality of user discernable indicators is
violated (pgs 2 and 4). ZoneAlarm is able to govern different sets of classes. Those
classes are outgoing traffic, incoming traffic, identifying/privacy data, and malicious
code. Examiner interprets these different categories of protection as classes.
ZoneAlarm protects the user from each of these types of classes, each posing their own
unique type of threat to a user and his/her network. What is unique about ZoneAlarm is
that each type of classes has its own set of rules governing those specific classes.
Certain classes can have higher levels of protection and can even break down those
classes into zones whereby different rules can be applied to the different zones. For
example, one could block all inbound traffic from an internet zone, and allow all inbound
traffic from a trusted zone. ZoneAlarm also provides different visual indicators for when
rules are broken for each type of class. The indicators themselves are unique to each
class and are color coded. For example in Figure 3, on page 2, an inbound threat
trigger is shown displayed in red. On page 4, in figure 7, an outbound threat trigger is
displayed in Orange. Another unique visual indicator is shown on page 4, in figure 8 as
a response to a privacy threat trigger. ZoneAlarm is silent in explicitly disclosing the
rules in the set are prioritized such that each of the plurality of classes represents a
respective different one of a plurality of priority levels. In an effort to only interrupt a

system administrator with the utmost critical alerts, Hrabik teaches a firewall system in

which the threats are prioritized and put into classes whereby only the higher classes

are immediately sent to a system engineer for responsive actions (0060). Hrabik

classifies threats but the security risk to the network. Moreover, the higher the risk then

the higher the importance of response. This feature would improve help a system

admin by prioritizing only the most critical threats allowing him/her to see the most

important alerts. And secondly it would also allow the reports to be categorized so that

the admin is not reading over pages of information looking for the important events that

have been logged. Simply, putting categorizing the threats make managing the system

more efficient. Therefore it would have been obvious to one of ordinary skill in the art at

the time of the invention to combine the priority levels of the rules into ZoneAlarm

because it would improve its efficiency.

As per claim 6, ZoneAlarm teaches one visual indicator comprises a highlighted

icon (alert to admin) displayed on a computing device (figure 7).

As per claim 7, ZoneAlarm teaches a method, comprising:

defining a set of rules to detect inappropriate communication activity on a computer or

network (see Figure 1); separating the rules in the set into a plurality of classes [classes

are outgoing traffic, incoming traffic, identifying/privacy data, and malicious code];

associating each of the plurality of classes with a different one of a plurality of user

discernable indicators; examining data traffic to determine whether at least one of the

rules has been violated; and in the case that at least one of the rules of a first one of

said plurality of classes has been violated, filtering said data traffic violating the at least

one of the rules of the first one of said plurality of classes, providing a user discernable

notification of said violation by triggering a respective one of the plurality of user

discernable indicators associated with the first one of said plurality of classes.

ZoneAlarm is able to govern different sets of classes. Those classes are outgoing

traffic, incoming traffic, identifying/privacy data, and malicious code. Examiner

interprets these different categories of protection as classes. ZoneAlarm protects the

user from each of these types of classes, each posing their own unique type of threat to

a user and his/her network. What is unique about ZoneAlarm is that each type of

classes has its own set of rules governing those specific classes. Certain classes can

have higher levels of protection and can even break down those classes into zones

whereby different rules can be applied to the different zones. For example, one could

block all inbound traffic from an internet zone, and allow all inbound traffic from a trusted

zone. ZoneAlarm also provides different visual indicators for when rules are broken for

each type of class. The indicators themselves are unique to each class and are color

coded. For example in Figure 3, on page 2, an inbound threat trigger is shown

displayed in red. On page 4, in figure 7, an outbound threat trigger is displayed in

Orange. Another unique visual indicator is shown on page 4, in figure 8 as a response

to a privacy threat trigger. ZoneAlarm is silent in explicitly disclosing the rules in the set

are prioritized such that each of the plurality of classes represents a respective different

one of a plurality of priority levels. In an effort to only interrupt a system administrator

with the utmost critical alerts, Hrabik teaches a firewall system in which the threats are

prioritized and put into classes whereby only the higher classes are immediately sent to

a system engineer for responsive actions (0060). Hrabik classifies threats but the security risk to the network. Moreover, the higher the risk then the higher the importance of response. This feature would improve help a system admin by prioritizing only the most critical threats allowing him/her to see the most important alerts. And secondly it would also allow the reports to be categorized so that the admin is not reading over pages of information looking for the important events that have been logged. Simply, putting categorizing the threats make managing the system more efficient. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the priority levels of the rules into ZoneAlarm because it would improve its efficiency.

As per claim 8, ZoneAlarm is silent in disclosing determining if a first threshold level of rule violation has been exceeded prior to filtering said data traffic. ZoneAlarm does explicitly teach associating a threshold to a particular rule. However, Hrabik teaches determining if a first threshold level of rule violation has been exceeded prior to filtering said data traffic (0060). To reduce the number of false alarms, thresholds are a means to monitor events for suspicious activities. A single occurrence of a packet may not be anything harmful. However, if the occurrences start to add up quickly, that is a sign of a problem. Being able to determine a threshold also allows the system to detect benign traffic which is being used for malicious purposes. Having this ability strengthens the system. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the use of threshold determination in a

firewall to both not block normal traffic but to also block normal traffic being used maliciously.

As per claim 9, ZoneAlarm is silent in disclosing determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator. Hrabik teaches determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator (0059, 0060). Examiner supplies the same rationale for thresholds as relied upon in the rejection of claim 8.

As per claims 20 and 21, ZoneAlarm teaches the firewall filters any of the packets that violate the one or more rules irrespective of a number of the packets that violate the one or more rules and triggers the respective one of the plurality of user discernable indicators (the color coded alerts of figures 4 and 7). ZoneAlarm is silent in disclosing determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator. Hrabik teaches determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator (0059, 0060). Examiner supplies the same rationale for thresholds as relied upon in the rejection of claim 8.

As per claims 23 and 27, ZoneAlarm teaches each of the plurality of user discernable indicators except a particular one [system tray icon, from picture above] is associated with the respective different one of the plurality of classes, the particular one of the plurality of user discernable indicators being associated with an affirmative status that filtering is being contemporaneously performed for any of the packets that violate the one or more rules [color code class alert indication in figures 4 and 7], and wherein

the method further comprises filtering any of the packets that violate the one or more

rules [firewall filters traffic], and wherein the particular one of the plurality of user

discernable indicators is concurrently triggered, along with the respective one of the

plurality of user discernable indicators, to indicate that the filtering is being

contemporaneously performed. Any one of ordinary skill in the art who has used

ZoneAlarm knows that whenever traffic is being filtered the little system tray icon

pictured above blinks to indicate traffic has been filtered. High level alerts or new alerts

get the larger pop up indication as shown in figures 4 and 7. Examiner is interpreting

the particular indicator equivalent to the small system tray icon of ZoneAlarm and the

user discernable indicators as the larger popup window alerts (having color coded

windows). It begs to reason that if a known rule is broken happens around the same

time as a newly detected threat, both icons would be perceived to occur at the same

time. In addition, ZoneAlarm continues to filter events while waiting for user interaction

on the newly detected threats. ZoneAlarm is silent in disclosing that a threshold must

first be exceeding before showing this indication. However, Hrabik teaches determining

if a first threshold level of rule violation has been exceeded prior to filtering said data

traffic (0060). To reduce the number of false alarms, thresholds are a means to monitor

events for suspicious activities. A single occurrence of a packet may not be anything

harmful. However, if the occurrences start to add up quickly, that is a sign of a problem.

Being able to determine a threshold also allows the system to detect benign traffic

which is being used for malicious purposes. Having this ability strengthens the system.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the

invention to combine the use of threshold determination in a firewall to both not block normal traffic but to also block normal traffic being used maliciously.

As per claims 24 and 28, Examiner supplies the same rationale for combining the threshold functionality of Hrabik into ZoneAlarm. ZoneAlarm teaches only the particular one of the plurality of user discernable indicators [small system tray icon] is triggered if the one or more of the rules is violated and the filtering is performed by the firewall program. Again, ZoneAlarm uses know that one can tell the system to only display the particular little system tray icon as shown in the picture above for events that are filtered and are already known about.

As per claims 25 and 29, Examiner supplies the same rationale for combining the threshold functionality of Hrabik into ZoneAlarm. ZoneAlarm teaches only the particular one of the plurality of user discernable indicators [small system tray icon] is triggered if the one or more of the rules is violated and the filtering is performed by the firewall program. Again, ZoneAlarm users know that one can tell the system to only display the particular little system tray icon as shown in the picture above for events that are filtered and are already known about. Examiner reiterates the conflict in interpreting the scope of this claim. Having only the respective one of the indicators triggers seems to be in disagreement with the parent claim which states the particular indicators always triggers on the first instance of a rule break.

As per claim 26, Examiner relies upon the same rationale as supplied in the rejection of claim 1. Hrabik teaches the priority levels of the threat determine the countermeasure (0060).

As per claim 30, Examiner relies upon the same rationale as supplied in the rejection of claim 7. Hrabik teaches the priority levels of the threat determine the countermeasure (0060).

As per claim 35, ZoneAlarm classifies threats into zones. Hrabik teaches that each zone of the network can be attributed its own priority when determining the threat level (0060). In relying on the combination of ZoneAlarm and Hrabik as recited in the rejection of claim 1, it naturally follows that each zone would have its own priority scheme. It is inherent from reading the teaching of Hrabik that the system engineer must be responsible for setting the threshold levels. It would have been necessary to include this feature with combination of ZoneAlarm and Hrabik for the system to work as intended.

Claims 16, 18, 19, 22, 31-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over ZoneAlarm in view of Hrabik and in view of USP 6,185,624B1 to Fijolek et al, hereinafter Fijolek.

As per claim 16, ZoneAlarm teaches a firewall program including a set of rules for identifying packets associated with inappropriate activity, the rules being separated into a plurality of classes, said firewall program being resident in said memory and

executable by said controller to cause examining data of packets from said downstream
and upstream circuitry; and a plurality of user discernable indicators, wherein each of
the plurality of user discernable indicators is associated with a different one of the
plurality of classes [classes are outgoing traffic, incoming traffic, identifying/privacy data,
and malicious code], and wherein a respective one of said plurality of user discernable
indicators (Figures 4 and 7) is triggered if one or more of the rules corresponding to one
of said plurality of classes associated with the respective one of said plurality of user
discernable indicators is violated. ZoneAlarm is able to govern different sets of classes.
Those classes are outgoing traffic, incoming traffic, identifying/privacy data, and
malicious code. Examiner interprets these different categories of protection as classes.
ZoneAlarm protects the user from each of these types of classes, each posing their own
unique type of threat to a user and his/her network. What is unique about ZoneAlarm is
that each type of classes has its own set of rules governing those specific classes.
Certain classes can have higher levels of protection and can even break down those
classes into zones whereby different rules can be applied to the different zones. For
example, one could block all inbound traffic from an internet zone, and allow all inbound
traffic from a trusted zone. ZoneAlarm also provides different visual indicators for when
rules are broken for each type of class. The indicators themselves are unique to each
class and are color coded. For example in Figure 3, on page 2, an inbound threat
trigger is shown displayed in red. On page 4, in figure 7, an outbound threat trigger is
displayed in Orange. Another unique visual indicator is shown on page 4, in figure 8 as
a response to a privacy threat trigger. ZoneAlarm is silent in explicitly disclosing the

rules in the set are prioritized such that each of the plurality of classes represents a respective different one of a plurality of priority levels. In an effort to only interrupt a system administrator with the utmost critical alerts, Hrabik teaches a firewall system in which the threats are prioritized and put into classes whereby only the higher classes are immediately sent to a system engineer for responsive actions (0060). Hrabik classifies threats but the security risk to the network. Moreover, the higher the risk then the higher the importance of response. This feature would improve help a system admin by prioritizing only the most critical threats allowing him/her to see the most important alerts. And secondly it would also allow the reports to be categorized so that the admin is not reading over pages of information looking for the important events that have been logged. Simply, putting categorizing the threats make managing the system more efficient. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the priority levels of the rules into ZoneAlarm because it would improve its efficiency.

ZoneAlarm firewall software is shown running a PC. A PC has memory, processors (controller), downstream circuits, upstream circuits. ZoneAlarm is silent though of implementing the program inside of a cable modem. Fijolek teaches that his cable modem has management software whereby an admin can program it via a network. One skilled in the art could see that the cable modem of Fijolek can perform the functionality of ZoneAlarm's firewall. One of ordinary skill in the art would have reasonable expectations of success and be motivated to protect the network from end to end. Therefore it would have been obvious to one of ordinary skill in the art at the

time of the invention to modify the teachings of Shanklin with the teaching of Fijolek;

namely to implement a firewall program within a cable modem.

As per claim 18, ZoneAlarm teaches plurality of user discernable indicators

comprises a first LED for signifying a filtering event (Figure 4 and 7) and a second LED

for signifying filtering data packets deemed pernicious in said set of rules. Also see

figure 6 for other alerts displayed. Anyone skilled in the art having used ZoneAlarm

knows that in the system tray icon a small alert shows when traffic is being filtered.

Here is a picture of that icon in the third row.

System Tray icons

The icons displayed in the system tray let you monitor your security status and Internet activity as frequently as you wish, and access your security settings in just a few clicks. Right-click any of the icons below to access a shortcut menu.

Icon	Description
	Zone Labs security software is installed and running.
	Your computer is sending (red band) or receiving (green band) network traffic. This does not imply that you have a security problem, or that the network traffic is dangerous.
	Zone Labs security software has blocked a communication, but your settings prevent a full-sized alert from being shown.
	(Yellow lock) The Internet Lock is engaged.
	(Red lock) The Stop button is engaged. You may also begin to see a lot of alerts.

Table 2-3: System Tray Icons

New and improved features in ZoneAlarm Pro version 3.0:

- Redesigned interface with all-new help system, quick-start tutorial, quick-reference text column, security overview panel and color-selectable interface

- Improved trusted security engine is further hardened and tamper-resistant

- New program component control to prevent abuse of trusted programs

- Optional program learning mode for easy set-up

- Optional program component learning mode for easy set-up

- New Zone management area makes keeping track of networks and computers quicker and easier

- Enhanced automatic network detection with wireless network identification and support

- New active network indicator shows what networks are active in what Zone

- Privacy protection: Cookie control, third-party spying control, Web bug and referrer header control, mobile code control

- Ad blocking: Granular ad blocking including pop-up/pop-under ad blocking, banner ad blocking, animation ad blocking, performance-based banner ad blocking (blocks only banner ads that slow Web page loads)

- New in-client logging with log filtering and sorting

- **New alert filtering: see all alerts, only high-rated alerts or no alerts**

- All new alert advisor with instant security advice from the experts at Zone Labs

- New IP address mapping to locate potential attackers from anywhere in the world

As per claim 19, ZoneAlarm teaches one visual indicator comprises a highlighted icon (alert message sent to admin) displayed on a computer device (figures 4 and 7).

As per claim 22, ZoneAlarm teaches the firewall filters any of the packets that violate the one or more rules irrespective of a number of the packets that violate the one or more rules and triggers the respective one of the plurality of user discernable indicators (the color coded alerts of figures 4 and 7). ZoneAlarm is silent in disclosing determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator. Hrabik teaches determining if a first threshold level of rule violation has been exceeded prior to triggering the user discernable indicator (0059, 0060). Examiner supplies the same rationale for thresholds as relied upon in the rejection of claim 8.

As per claim 31, ZoneAlarm teaches each of the plurality of user discernable indicators except a particular one [system tray icon, from picture above] is associated with the respective different one of the plurality of classes, the particular one of the plurality of user discernable indicators being associated with an affirmative status that filtering is being contemporaneously performed for any of the packets that violate the one or more rules [color code class alert indication in figures 4 and 7], and wherein the method further comprises filtering any of the packets that violate the one or more rules [firewall filters traffic], and wherein the particular one of the plurality of user discernable indicators is concurrently triggered, along with the respective one of the plurality of user discernable indicators, to indicate that the filtering is being contemporaneously performed. Any one of ordinary skill in the art who has used ZoneAlarm knows that whenever traffic is being filtered the little system tray icon pictured above blinks to indicate traffic has been filtered. High level alerts or new alerts get the larger pop up indication as shown in figures 4 and 7. Examiner is interpreting the particular indicator equivalent to the small system tray icon of ZoneAlarm and the user discernable indicators as the larger popup window alerts (having color coded windows). It begs to reason that if a known rule is broken happens around the same time as a newly detected threat, both icons would be perceived to occur at the same time. ZoneAlarm is silent in disclosing that a threshold must first be exceeding before showing this indication. However, Hrabik teaches determining if a first threshold level of rule violation has been exceeded prior to filtering said data traffic (0060). To reduce the number of false alarms, thresholds are a means to monitor events for suspicious activities. A

single occurrence of a packet may not be anything harmful. However, if the

occurrences start to add up quickly, that is a sign of a problem. Being able to determine

a threshold also allows the system to detect benign traffic which is being used for

malicious purposes. Having this ability strengthens the system. Therefore it would

have been obvious to one of ordinary skill in the art at the time of the invention to

combine the use of threshold determination in a firewall to both not block normal traffic

but to also block normal traffic being used maliciously.

As per claim 32, Examiner supplies the same rationale for combining the

threshold functionality of Hrabik into ZoneAlarm. ZoneAlarm teaches only the particular

one of the plurality of user discernable indicators [small system tray icon] is triggered if

the one or more of the rules is violated and the filtering is performed by the firewall

program. Again, ZoneAlarm uses know that one can tell the system to only display the

particular little system tray icon as shown in the picture above for events that are filtered

and are already known about.

As per claim 33, Examiner supplies the same rationale for combining the

threshold functionality of Hrabik into ZoneAlarm. ZoneAlarm teaches only the particular

one of the plurality of user discernable indicators [small system tray icon] is triggered if

the one or more of the rules is violated and the filtering is performed by the firewall

program. Again, ZoneAlarm users know that one can tell the system to only display the

particular little system tray icon as shown in the picture above for events that are filtered

and are already known about. Examiner reiterates the conflict in interpreting the scope

of this claim. Having only the respective one of the indicators triggers seems to be in

disagreement with the parent claim which states the particular indicators always triggers on the first instance of a rule break.

As per claim 34, Examiner relies upon the same rationale as supplied in the rejection of claim 16. Hrabik teaches the priority levels of the threat determine the countermeasure (0060).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am

- 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2431